UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/766,337	01/27/2004	Derek L. Davis	42P6514C	3287

7590 09/11/2008

Blakely, Sokoloff, Taylor & Zafman LLP
7th Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
FIELDS, COURTNEY D	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
09/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.**	**Applicant(s)**	
	10/766,337	DAVIS, DEREK L.	
	Examiner	**Art Unit**	
	COURTNEY D. FIELDS	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 June 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-11,13-19 and 22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-11,13-19 and 22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 2-11, 14-19, and 22 are pending.

Response to Arguments

1. Applicant's arguments filed 16 June 2008 have been fully considered but they are not persuasive.

2. Referring to the rejection of claim 2, the Applicant contends that the prior art, Perlman, Krawczyk, and Taylor, taken alone or in any combination do not disclose, suggest or teach, generating an integrity check value by the first device comprising: extracting a selected number of bits from a pseudo-random data stream for use as coefficients of a matrix having M rows and N columns, and performing operations on both contents of the message and the coefficients of the matrix to generate the integrity check value.

The Examiner respectfully disagrees and asserts that Perlman et al. discloses a method for establishing a shared secret between parties communicating over a network. The remote device (first device) and the user's local device (second device) are mutually authenticated, once the communication is secure, an integrity check value is performed which may be used to encrypt data (See Column 4, lines 42-64)

The Examiner respectfully disagrees and asserts that Krawczyk discloses the use of toeplitz matrices for extracting bits randomly for use as coefficients of a matrix having M rows and N columns and performing operations to generate the integrity check value for hash messages (See pages301- 303) The toeplitz matrices performs operations on both the content of the hash message as well as the coefficients which are the random bits used to generate a sequence (See page 303)

3. Referring to the rejection of claim 18, the Applicant contends that the prior art, Perlman do not disclose, suggest or teach, generating an integrity check value, producing the integrity check value based on a selected group of bits from a pseudo-random data stream and contents of the message. The Examiner respectfully disagrees and asserts that in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

3. Furthermore, as shown in the previous office action, the Examiner clearly points out that Krawczyk discloses generating an integrity check value, producing the integrity check value based on a selected group of bits from a pseudo-random data stream and contents of the message as shown on page 308, Section 4 and page 309, 1st and 2nd paragraph.

4. Referring to the rejection of claim 13, the Applicant contends that the prior art, Perlman nor Krawczyk do not disclose, suggest or teach, decrypting an incoming message, computing an integrity check value for an incoming message and determining whether the incoming message is valid by comparing the computed integrity check value with the recovered integrity check value. The Examiner respectfully disagrees and asserts that in response to applicant's arguments against the references individually,

one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

5. Furthermore, as shown in the previous office action, the Examiner clearly points out that Taylor discloses decrypting an incoming message (See Column 10, lines 66-67, Column 11, line 1, and Column 17, line 2), computing an integrity check value for an incoming message (See Column 11, lines 1-7 and Column 17, lines 1-2) and determining whether the incoming message is valid by comparing the computed integrity check value with the recovered integrity check value (See Column 11, lines 7-14 and Column 16, lines 66-67)

6. Therefore, the rejection of claims 2-11, 14-19, and 22 are maintained in view of the reasons above and in view of the reasons below.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 2-11, 14-19, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al. (US Patent No. 6,173,400) in view of Krawczyk, Hugo "New Hash Functions for Message Authentication".

As per claim 2, Perlman et al. discloses a method for securing communications between a first device and a second device comprising:

mutually authenticating the first device and the second device (See Column 4, lines 42-64),

generating an integrity check vale by the first device (See Column 4, lines 42-64),

and sending the integrity check value with a message from the first device to the second device (See Column 4, lines 42-64),

However, Perlman et al. does not explicitly disclose the feature of extracting bits from a pseudo-random data stream for use in a matrix having M rows and N columns. Krawczyk teaches a method and system which uses Toeplitz matrices.

Krawczyk discloses the claimed limitation of extracting bits randomly for use as coefficients of a matrix having M rows and N columns and performing operations to generate the integrity check value. (See pages 301-303)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Perlman et al.'s shared secret system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to gain the advantage of using a Toeplitz matrix as opposed to purely random bits that the former can generate efficiently out of a short random seed (See Krawczyk, page, 308, Section 4)

As per claim 3, (Perlman et al. as modified by Krawczyk) discloses the claimed limitation of inputting keying material into a cipher engine performing operations in accordance with a stream cipher and producing the pseudo-random stream by the cipher engine. (See Krawczyk, page 302)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Perlman et al.'s shared secret system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to gain the advantage of using a Toeplitz matrix as opposed to purely random bits that the former can generate efficiently out of a short random seed (See Krawczyk, page, 308, Section 4)

As per claim 4, (Perlman et al. as modified by Krawczyk) discloses the claimed limitation wherein a counter mode stream cipher in Data Encryption Standard. (See Krawczyk, page 304, Section 2.2, 1st and 2nd paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Perlman et al.'s shared secret system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to gain the advantage of using a Toeplitz matrix as opposed to purely random bits that the former can generate efficiently out of a short random seed (See Krawczyk, page, 308, Section 4)

As per claims 5 and 9, (Perlman et al. as modified by Krawczyk) discloses the claimed limitation of assigning M bits from the selected number of bits as a first column of the matrix and assigning M bits for each remaining column of the matrix. (See Krawczyk, page 307)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Perlman et al.'s shared secret system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to gain the advantage of using a Toeplitz matrix as opposed to purely random bits that the former can generate efficiently out of a short random seed (See Krawczyk, page, 308, Section 4)

As per claims 6 and 10, (Perlman et al. as modified by Krawczyk) discloses the claimed limitation of performing arithmetic operations on M bits from the content of the message and coefficients of the first column of the matrix and performing an exclusive OR operation between each of the values to produce integrity check value. (See Krawcyk, page 304, Section 2.2, 1st paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Perlman et al.'s shared secret system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to gain the advantage of using a Toeplitz matrix as opposed to purely random bits that the former can generate efficiently out of a short random seed (See Krawczyk, page, 308, Section 4)

As per claim 7, (Perlman et al. as modified by Krawczyk) discloses the claimed limitation wherein the arithmetic operations are bitwise multiplication operations. (See Krawcyk, page 304, Theorem 3, and 3rd paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Perlman et al.'s shared secret system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to gain the advantage of using a Toeplitz matrix as opposed to purely random bits that the former can generate efficiently out of a short random seed (See Krawczyk, page, 308, Section 4)

As per claim 8, (Perlman et al. as modified by Krawczyk) discloses the claimed limitation of performing arithmetic operations on the M bits from the message for a N-1 column of the matrix and performing exclusive OR operations between values associated with N-1 column of the matrix to produce N-1 bits of the integrity check value. (See Krawcyk, page 307, Section 3)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Perlman et al.'s shared secret system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to gain the advantage of using a Toeplitz matrix as opposed to purely random bits that the former can generate efficiently out of a short random seed (See Krawczyk, page, 308, Section 4)

As per claims 11 and 17, (Perlman et al. as modified by Krawczyk) discloses the claimed limitation of computing the integrity check value based on bits in the message, and determining if the bits differ from the predetermined bits set for the integrity check value. (See Krawcyk, page 309)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Perlman et al.'s shared secret system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to gain the advantage of using a Toeplitz matrix as opposed to purely random bits that the former can generate efficiently out of a short random seed (See Krawczyk, page, 308, Section 4)

As per claims 14, 15, and 16, (Perlman et al. as modified by Krawczyk) discloses the claimed limitation of performing arithmetic operations on M bits from the content of the message and coefficients of the first column of the matrix and performing an exclusive OR operation between each of the values to produce integrity check value. (See Krawcyk, page 304,1st and 2nd paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Perlman et al.'s shared secret system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to gain the advantage of using a Toeplitz matrix as opposed to purely random bits that the former can generate efficiently out of a short random seed (See Krawczyk, page, 308, Section 4)

As per claim 18, (Perlman et al. as modified by Krawczyk) discloses the claimed limitation the first device includes a integrity check value generator to produce an integrity check value based on a selected group of its from a pseudo-random data stream and contents of the message. (See Krawczyk, page 308, Section 4 and page 309,1st and 2nd paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Perlman et al.'s shared secret system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to gain the advantage of using a Toeplitz matrix as opposed to purely random bits that the former can generate efficiently out of a short random seed (See Krawczyk, page, 308, Section 4)

As per claims 19 and 22, (Perlman et al. as modified by Krawczyk) discloses the claimed limitation wherein the first device is a processor (See Perlman et al., Column 5, line 6) and the second device is a memory (See Perlman et al., Column 5, line 6)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Perlman et al.'s shared secret system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to gain the advantage of using a Toeplitz matrix as opposed to purely random bits that the former can generate efficiently out of a short random seed (See Krawczyk, page, 308, Section 4)

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al. (US Patent No. 6,173,400) and Krawczyk, Hugo “New Hash Functions for Message Authentication” as applied to claims 2-11, 14-19, and 22 above, and further in view of Taylor (US Patent No. 5,703,952). As per claim 2, Perlman et al. discloses the invention as substantially claimed.

However, neither Perlman et al. nor Krawczyk explicitly disclose the feature of decrypting an incoming message, computing an integrity check value for an incoming message and determining whether the incoming message is valid by comparing the computed integrity check value with the recovered integrity check value.

Taylor discloses a system for encrypting or decrypting a digital message for generating a cipher stream.

As per claim 13, (Perlman et al. and Krawczyk as modified by Taylor) discloses a method comprising:

decrypting an incoming message (See Taylor, Column 10, lines 66-67, Column 11, line 1 and Column 17, line 2),

computing an integrity check value for an incoming message (See Taylor, Column 11, lines 1-7 and Column 17, lines 1-2)

and determining whether the incoming message is valid by comparing the computed integrity check value with the recovered integrity check value (See Taylor, Column 11, lines 7-14 and Column 16, lines 66-67)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Perlman et al.'s shared secret system and Krawczyk's hash function for message authentication by combining Taylor's cipher stream system. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to provide integrity checking which prevents such alterations during transmission from taking place without detection of the cipher text (See Taylor, Column 2, lines 7-26)

Conclusion

2. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to COURTNEY D. FIELDS whose telephone number is (571)272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Courtney D. Fields/
Examiner, Art Unit 2137
September 9, 2008

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137